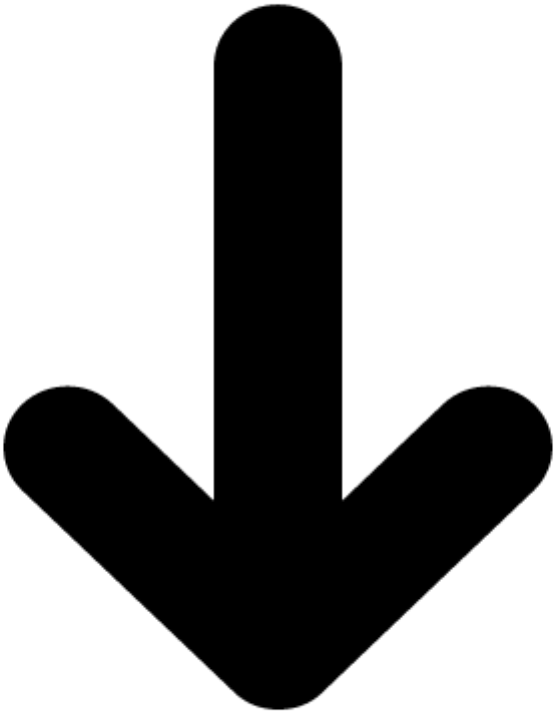
Proyek 6: Implementasi IDS (Intrusion Detection System) dengan Snort / Suricata

Nama Kelompok :

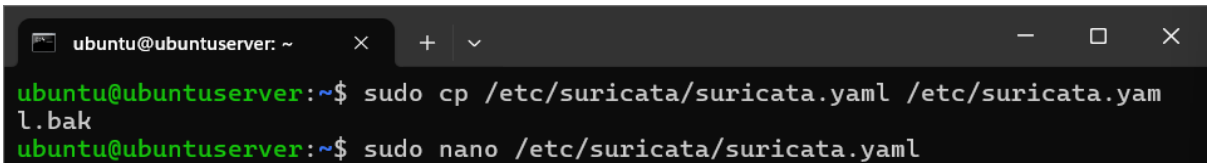
- 2201020098 Muhammad Rifqi
- 2201020123 Handicap
- 2201020139 Muhammad Iqbal Hordani
- 2201020101 Irsyad Widiansyah



Konfigurasi interface & basic rules Suricata

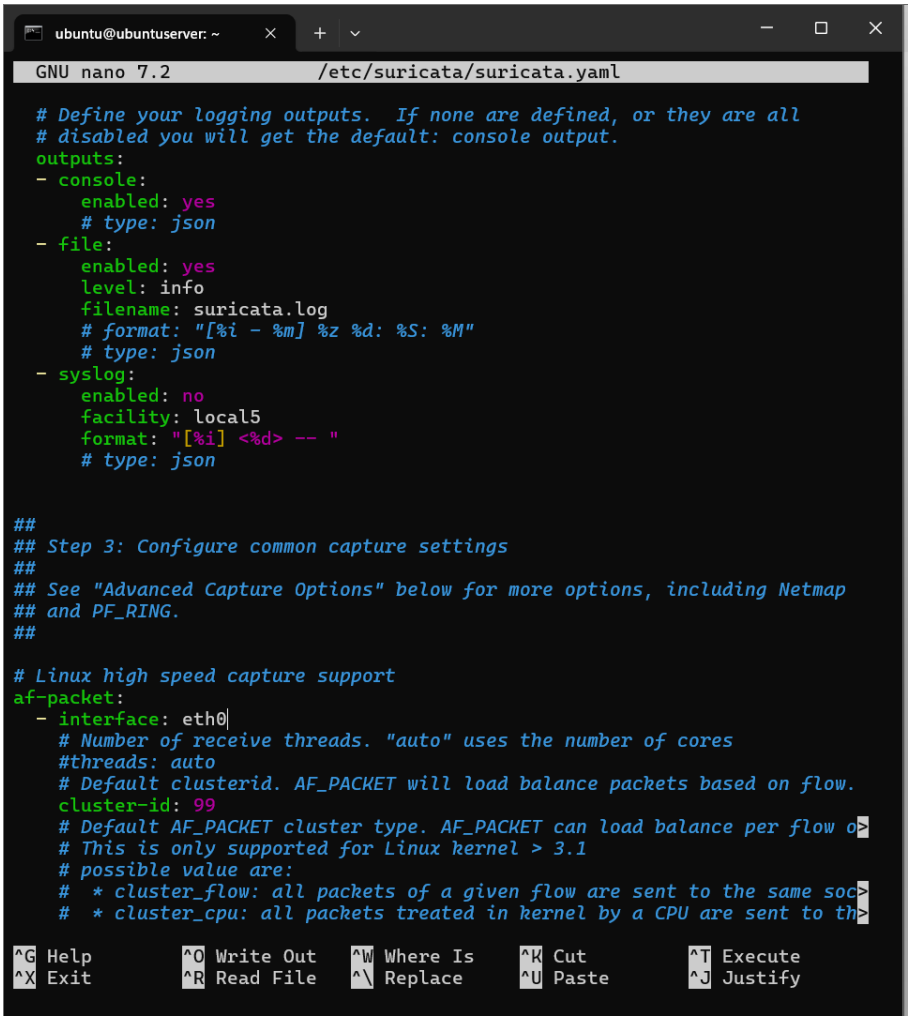
*Konfigurasi

1. sudo cp /etc/suricata/suricata.yaml /etc/suricata.yaml.bak



Melakukan backup file konfigurasi default Suricata (Langkah ini dilakukan untuk memastikan bahwa konfigurasi asli tetap aman apabila suatu saat diperlukan pemulihan.)

2. sudo nano /etc/suricata/suricata.yaml (Edit section af-packet interface:enps0s8)

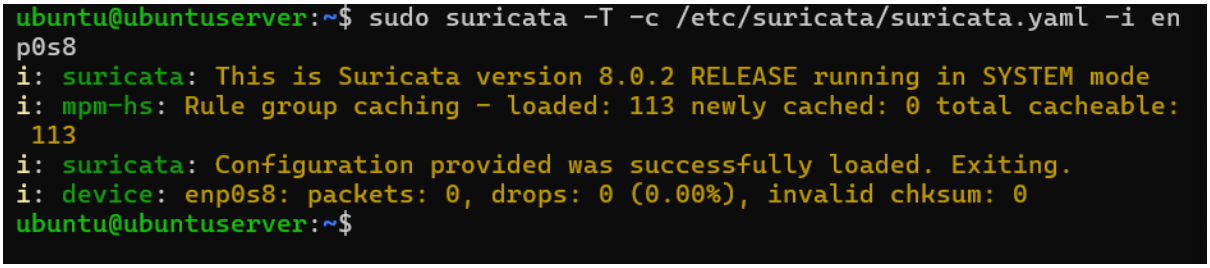


Melakukan pengeditan file suricata.yaml untuk menyesuaikan interface jaringan yang akan dipantau. (Pada bagian af-packet, interface diubah menjadi enp0s8 agar Suricata menangkap lalu lintas pada interface tersebut.)

3. sudo mkdir -p /var/log/suricata
4. sudo chmod 755 /var/log/suricata
5. sudo chown suricata:suricata /var/log/suricata

- Membuat direktori log Suricata (sudo mkdir -p /var/log/suricata) Direktori ini digunakan sebagai lokasi penyimpanan seluruh output log dari Suricata.
- Mengatur permissions direktori log (sudo chmod 755 /var/log/suricata sudo chown suricata:suricata /var/log/suricata) Langkah ini memastikan Suricata memiliki hak akses penuh untuk menulis log ke direktori tersebut.

6. sudo suricata -T -c /etc/suricata/suricata.yaml -I enp0s8 (test configuration)



Melakukan pengujian konfigurasi (Perintah ini berfungsi untuk memeriksa apakah file konfigurasi sudah benar. Jika muncul pesan *"Configuration provided was successfully loaded"*, maka konfigurasi berhasil dan tidak terdapat error.)

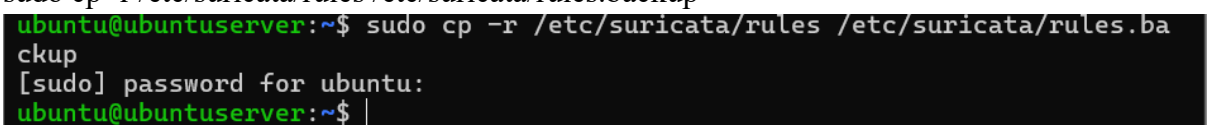
*basic rules Suricata

*Rule

1. alert tcp any any -> $HOME_NET any (msg:"[SURICATA] Port Scan Terdeteksi"; flags:S; threshold:type threshold, track by_src, count 5, seconds 3; sid:1000001; rev:1;)
(Rule ini akan memicu alert apabila terdapat 5 koneksi SYN dalam waktu 3 detik dari satu sumber yang sama, yang biasanya mengindikasikan aktivitas port scanning.)

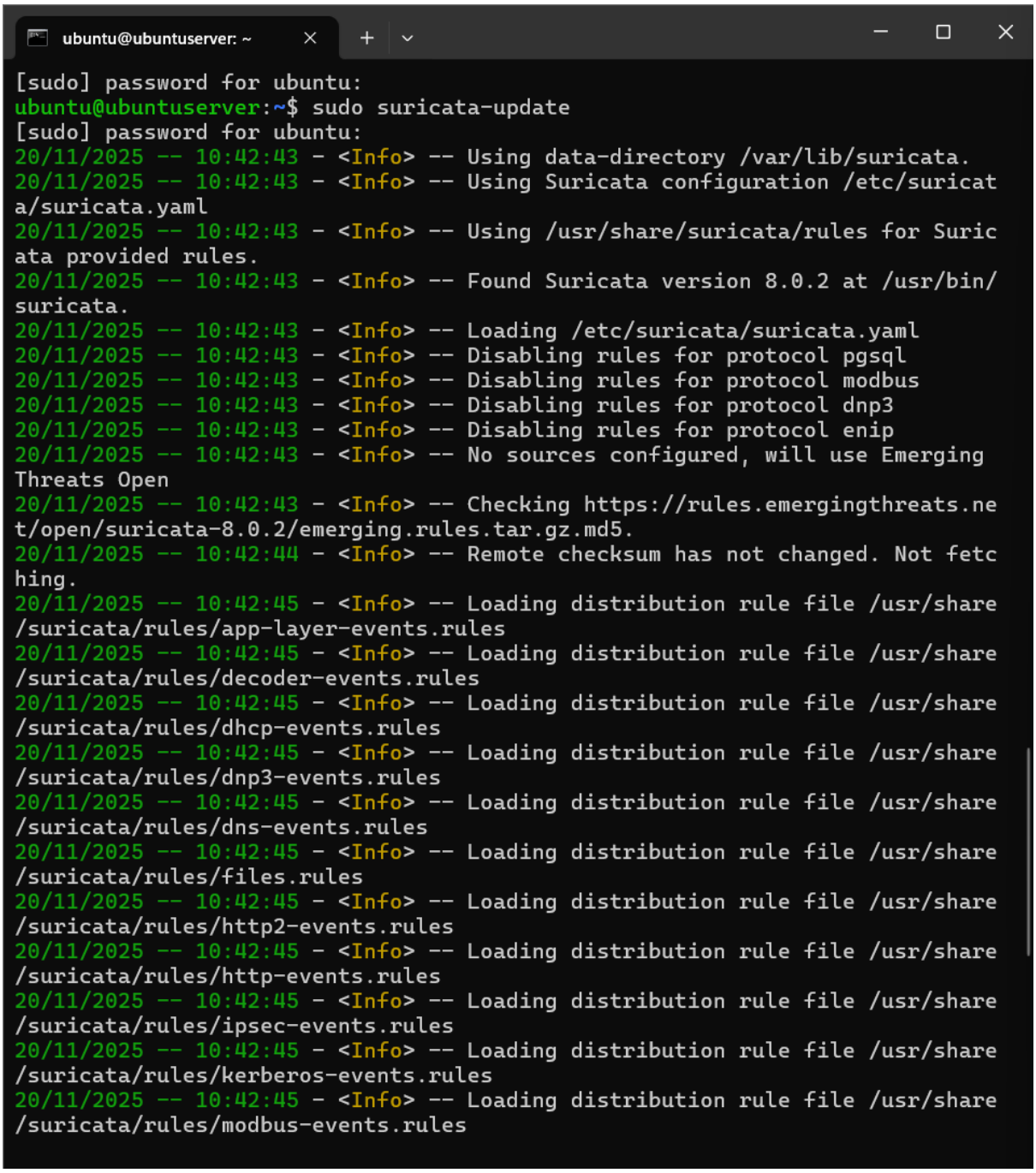
2. alert tcp any any -> $HOME_NET 22 (msg:"[ALERT] Banyak Koneksi ke SSH - Kemungkinan brute-force"; flags:S; threshold:type both, track by_src, count 5, seconds 60; sid:1000004; rev:1;)
(Rule ini mendeteksi adanya banyak koneksi menuju port SSH (22) dalam waktu singkat, yang merupakan ciri serangan brute-force login.)

1. sudo cp -r /etc/suricata/rules /etc/suricata/rules.backup



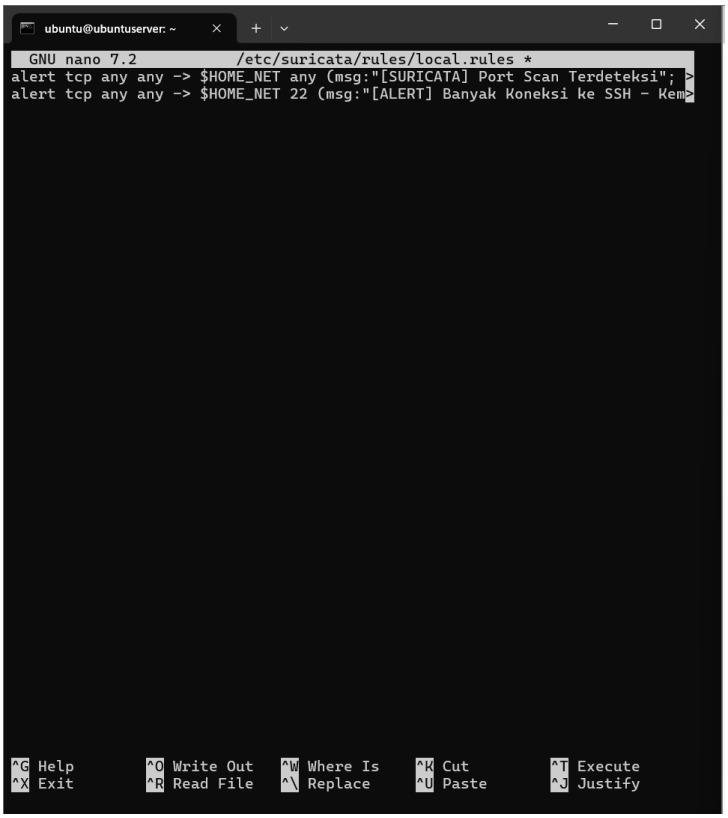
(Membuat backup folder rules)

2. sudo suricata-update



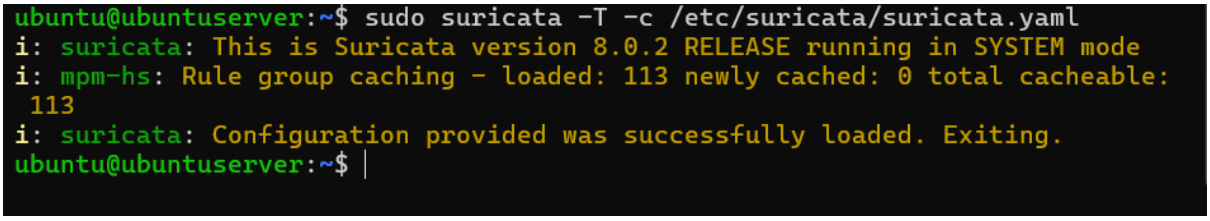
Mengupdate rules Suricata (Tahapan ini digunakan untuk memperbarui rule-rule dari komunitas (ET Open Rules).)

3. sudo nano /etc/suricata/rules/local.rules



Menambahkan rule local (Pada file inilah kedua rule yang telah dibuat sebelumnya disimpan.)

4. sudo suricata -T -c /etc/suricata/suricata.yaml



Melakukan pengujian konfigurasi Kembali (Pengujian ini memastikan rule lokal dan konfigurasi Suricata sudah benar dan siap digunakan.)